IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS 1465 HOOKSETT ROAD #1358, HOOKSETT, NH DESCRIBED FULLY IN ATTACHMENT A, INCLUDING VEHICLES LOCATED THEREON, AND THE PERSON OF STUART ADAMS	Case No. 20-mj- 213-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Tarah Rankins, a Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state as follows: I have been employed as an FBI Special Agent since 2015, and am currently assigned to the Boston Field Office, Bedford Resident Agency. I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 1470, and I am authorized by the Attorney General to request a search warrant. While employed by the FBI, I have investigated criminal violations relating to crimes against persons utilizing the internet, the sexual exploitation and trafficking of minor children through the internet, child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography. I have received training in the area of internet crimes against persons, sexual exploitation and trafficking of minor children through the internet, child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of venues individuals utilize to advertise and exploit minor children for sexual encounters via the internet as well as child pornography in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of

which involved internet crimes against persons, sex trafficking of minors, child exploitation and/or child pornography offenses.

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at **1465 Hooksett Road #1358, Hooksett, NH** (hereafter "SUBJECT PREMISES"), further described in Attachment A, one 2020 gray Chevrolet Silverado with New Hampshire registration number 0 and the person of Stuart Lee Adams, and any computer, computer media, and electronic media located therein, for the things described in Attachment B – specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1470, which relates to the transfer and attempted transfer of obscene material to minors.

2. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

3. This investigation concerns alleged violations of 18 U.S.C. § 1470, which makes it a crime for anyone, using the mail or any facility or means of interstate or foreign commerce, to knowingly transfer or attempt to transfer obscene matter to another individual who has not

attained the age of 16 years, knowing that such other individual has not attained the age of 16 years.

DEFINITIONS

4. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and colocation of computers and other communications equipment. Many ISPs assign each subscriber an account name a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. ISPs maintain records ("lSP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

5. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or device to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

PROBABLE CAUSE

6. On August 22, 2020 a source who has previously provided reliable information to the FBI pertaining to online child exploitation offenses contacted the FBI regarding Kik, a

mobile application that allows users to send each other messages that include text, pictures and videos[1]. The source, who maintains a presence on Kik, stated that the Kik username " 3003", with a display name of Steve A ("SUSPECT KIK USER") and email address of " ahoo.com" was a 59 year-old male that expressed to the source an interest in chatting with underage females. On numerous occasions, the SUSPECT KIK USER requested that the source help him establish contact with minor females on the Kik platform.

7. On October 6, 2020, at the direction of the FBI, the source provided the SUSPECT KIK USER with the Kik username, the online persona of an FBI Online Undercover Employee ("OCE") portraying a 13-year-old girl. The OCE was engaged in an online operation designed to identify adults who were seeking out minors online for sexually explicit conduct. The source advised the SUSPECT KIK USER that was a 13-year-old girl named Madison living in the United States. Soon after, the OCE received a message on Kik from the SUSPECT KIK USER who introduced himself as "Steve." The SUSPECT KIK USER and OCE then chatted exclusively on the Kik messenger application. The SUSPECT KIK USER revealed to OCE that he lives in New Hampshire. OCE responded that she lives in Massachusetts.

[1] According to the publicly available "Kik's Guide for Law Enforcement", Kik is a smartphone messenger application that lets users connect with their friend and the world around them through chat. Users can send text, pictures, and videos and more – all within the app. Kik is available to download through iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can send each other text messages, images, and videos. "Kik's Guide for Law Enforcement" is available at https://lawenforcement.kik.com/hc/en-us//articles/360039841472-Law-Enforcement-Guide.

8. On October 8, 2020, the SUSPECT KIK USER says to OCE, "Good weather to cuddle. Hmm..come on over, we can cuddle".

9. On October 9, 2020, the SUSPECT KIK USER said, "So instead you should come over [Smiling Emoji]". OCE responded, "Aww I wish! How would I get there?!". The SUSPECT KIK USER replied, "Oh yeah, that would be tough for you. Long walk and or bike ride". On the same day, OCE stated, "I'm mature but still a dumb 13 year old lol [Blushing Emoji]". The SUSPECT KIK USER responded, "Oh but you're cool don't worry".

10. Later that same day, the SUSPECT KIK USER said, "Hi, got my hair cut [Smiling Emoji]" and immediately followed that text by sending a selfie picture of himself sitting in a black office chair and wearing a blue T-shirt. The SUSPECT KIK USER had gray hair and appeared to be approximately 60 years old.

11. On October 15, 2020, the SUSPECT KIK USER asked to see a picture of OCE. The OCE sent a picture that depicted a young female wearing a blue hooded sweatshirt, lying on her back.[2] The SUSPECT KIK USER replied, "Oh so pretty".

12. In the afternoon of October 15, 2020, the SUSPECT KIK USER and OCE had the following conversation:

SUSPECT KIK USER: Hmm, I'm back at my desk. No pants this time.

OCE: No????. [Surprised Emoji]. Boxers?

SUSPECT KIK USER: Sorta..boxerbriefs. Should I just those off too

OCE: Mmm

[2] This photograph depicts an FBI Special Agent. Because of the size and figure of the Special Agent, the angle and perspective of the photograph, the OCE used this photograph with the intention of it representing a 13-year-old female named Madison.

SUSPECT KIK USER: Should I

OCE: Errmmm….If u want to!! [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: Okay …slipping them off

OCE: [Smiling Emoji]

SUSPECT KIK USER: What about you?

OCE: Are they off?!

SUSPECT KIK USER: Yep

OCE: My mom is in the other room [Upset Emoji]

SUSPECT KIK USER: Oh okay..oops. What are you wearing now

OCE: No it's ok! I just can't rn [Disappointed Emoji]. Are urs really off?!

SUSPECT KIK USER: Yeah ..just in tshirt and socks

OCE: And what r u doin????

SUSPECT KIK USER: Chatting with you [Smiling Emoji]. What are you suggesting.

OCE: Lol that's it?? Idk. U have no pants [Blushing Emoji]

SUSPECT KIK USER: Well touching a little

OCE: [Smiling Blushing Emoji]

SUSPECT KIK USER: Oh….you like that

OCE: Maaayyyybe [Kiss Emoji]

SUSPECT KIK USER: Maybe?

OCE: Yessss

SUSPECT KIK USER: Oh my..thinking of you

OCE: Yea??

SUSPECT KIK USER: What if you were here

OCE: What r u thinking about?

SUSPECT KIK USER: Thinking about you touching me

OCE: [Smiling Emoji]

SUSPECT KIK USER: You told me you had only touched one guy

OCE: I would like that. Yes. Is that ok?

SUSPECT KIK USER: Good. Yes,it is

OCE: Ok phew

SUSPECT KIK USER: Would be nice

OCE: Is it hard??!

SUSPECT KIK USER: Yes very

OCE: [Surprised Emoji]

SUSPECT KIK USER: I'm bigger than your ex

OCE: Really?! I'm sure But he is just a boy. Only one I've seen [Sad Emoji]. I feel other girls in my grade have seen more.

SUSPECT KIK USER: Yes I'm sure. Why do you say that

OCE: Just what I've heard. Is it still hard????

SUSPECT KIK USER: Yes

OCE: [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: You want to see?

OCE: Errmmmm…..yesssssss

SUSPECT KIK USER: [Sends a picture of a naked adult erect penis from an overhead camera angle. The picture also depicts a tan rug/mat with a black and red checkered border on the floor.][3]

SUSPECT KIK USER: Only fir you

OCE: [Four Heart Emojis]

SUSPECT KIK USER: Oh you like it?

13. Also on October 15, 2020, the SUSPECT KIK USER amd OCE continued the conversation:

SUSPECT KIK USER: I'm really horny now lol

OCE: Awww lol

SUSPECT KIK USER: I wish you could feel

OCE: Sry my mom was just nagging me

SUSPECT KIK USER: lol, oh that happens

OCE: She was about to leave and tells me all this stuff like I'm a baby. I'm like Mom! I'm 13! I got it! Lol [Mad Emoji]

SUSPECT KIK USER: Oh wow, like what

OCE: Like don't answer the door blah blah blah

SUSPECT KIK USER: Okay..good

OCE: Bust she's gone now [Hands up Emoji]

SUSPECT KIK USER: Oh okay cool. What ya want to chat about

OCE: U tell me. Is ur wife home?

[3] This image is available for the Court's review.

SUSPECT KIK USER: No. I'm alone

OCE: [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: Hmm well I'm just here in a tshirt still

OCE: Reeeeaaally?

SUSPECT KIK USER: Yes really lol

OCE: R u touching it?

SUSPECT KIK USER: Yes. Is that ok. How your mom gone for. What ya doing

OCE: Yessss it is

SUSPECT KIK USER: Good

OCE: She went to the grocery store so [Shrug Emoji]

SUSPECT KIK USER: Hmm wanna take off your shorts and undies?

OCE: Is that what u want???

SUSPECT KIK USER: Yes. Be like me

OCE: Okkkkk!

SUSPECT KIK USER: Oh nice

OCE: Done!

SUSPECT KIK USER: Very nice. Should we get naked?

OCE: Do u want to???

SUSPECT KIK USER: [Sends a shirtless selfie picture showing face and bare chest, sitting in a black chair]

SUSPECT KIK USER: Lol not great pic

OCE: I luv it! [Two Kiss Face Emojis]

SUSPECT KIK USER: Wasn't sitting up straight. [Smile Emoji] Be naked with me

OCE: What do you want me to do?!

SUSPECT KIK USER: Are you naked

OCE: Yesssss

SUSPECT KIK USER: Oh wow very nice

OCE: Lol r u surprised?

SUSPECT KIK USER: Well I had asked you to. Nonetheless I like it

OCE: I'm a good listener I guess lol

SUSPECT KIK USER: Are you touching?

OCE: Errmm what do you want me to touch?

SUSPECT KIK USER: Touch your pussy, spread your leafs as you do

OCE: [Blushing Smiling Emoji] ok. Leafs?

SUSPECT KIK USER: Legs

OCE: Lol ohhh ok

SUSPECT KIK USER: You know how don't you [Smiling Emoji]

OCE: Errrmmm mayyybe [Blushing Smiling Emoji]

SUSPECT KIK USER: Rub your finger along your opening. Feels good?

OCE: Ok. Yesssss. R u touching?

SUSPECT KIK USER: Yes mmm feels really good. Are you wet? I'm very hard

OCE: yesss

SUSPECT KIK USER: Mmm good. I wish you could feel me now

OCE: Meee too

SUSPECT KIK USER: You could rub me. I won't last long

OCE: Would I want me to?

SUSPECT KIK USER: If you wanted

OCE: Up to u!

SUSPECT KIK USER: Yes, I'd want you to

OCE: [Smiling Emoji with Heart Shaped Eyes]. Jus rub u?

SUSPECT KIK USER: Youu can do what you want then. Mmm Feels is good

OCE: What would I want me to do?

SUSPECT KIK USER: You could jerk me and watch me shoot

OCE: Mmmm I'd like that

SUSPECT KIK USER: Okay, you could watch me do it too

OCE: I'd like that too! What else??!

SUSPECT KIK USER: I could watch you. Hmm, could I kiss your pussy

OCE: Do what?

SUSPECT KIK USER: Kiss you're vagina and lick you there

OCE: Errmm I've never done that before. Will it hurt?

SUSPECT KIK USER: No, I wouldn't hurt you. I think you'd like it

OCE: Ok good

SUSPECT KIK USER: I'd lick you there

OCE: Mmm [Smiling Licking Emoji]

SUSPECT KIK USER: Mmm I'm stroking now…gonna cum soon

14. The SUSPECT KIK USER and OCE continued to chat on a nearly daily basis since October 6, 2020 with the SUSPECT KIK USER initiating the conversation each day. On October 20, 2020, OCE tells the SUSPECT KIK USER, "I jus hope next year when I'm in 8th grade we are back to school". The SUSPECT KIK USER responds, "I hope so too by then for sure".

15. On October 20, 2020, the SUSPECT KIK USER sent OCE a picture depicting an adult male, naked from the waist down with a naked penis displayed in the foreground. The adult male appears to be sitting down and wearing a white T-shirt.[4] The OCE explains that her mom is out running errands. The SUSPECT KIK USER asks when she will be home and then sends another picture of an adult male, wearing a white T-shirt, naked from the waist down holding an erect naked penis with his left hand.[5] The SUSPECT KIK USER then sends a short video of what appears to be the same adult male masturbating an erect naked penis.[6]

16. Later on October 20, 2020, the following conversation took place:

SUSPECT KIK USER: Do you have pjs on still

OCE: No silly u asked me to take them off! Lol

SUSPECT KIK USER: Mmm nice. Are you sitting at your desk

OCE: Yesss

SUSPECT KIK USER: Hmm…are you touching your kitty

OCE: Yesss

SUSPECT KIK USER: Mm nice

---

[4] This image is available for the Court's review.

[5] This image is available for the Court's review.

[6] This image is available for the Court's review.

OCE: Wait, I think so?? What's my kitty lol

SUSPECT KIK USER: I wish I could see. Between your legs

OCE: Ohhhh lol. I'm so stupid

SUSPECT KIK USER: Mmm it's cool…I wasn't sure what you called it

OCE: [Hand On Forehead Emoji]. What should I do next??

SUSPECT KIK USER: Are you wet

OCE: Yessss

SUSPECT KIK USER: Mmm nice madi. Run your finger along the opening

OCE: Okkkkk

SUSPECT KIK USER: Does it feel good

OCE: Yesssss. I wish u were here

SUSPECT KIK USER: Oh me too. Can I see your face now?

OCE: I'm really gross rn lol. Does it have to be my face?

SUSPECT KIK USER: It's okay, I wanna see. Are you in hoodie and tshirt still? Can I see the rest of you then

OCE: I took them off silly!

SUSPECT KIK USER: Oh wow, okay [Smiling Emoji]

OCE: [Smiling Blushing Emoji]

SUSPECT KIK USER: What can I see

OCE: What do u want to see????

SUSPECT KIK USER: Oh ..hmm your breasts

OCE: How should I do it??

SUSPECT KIK USER: Can you just do a selfie pic

OCE: Of my breasts?

SUSPECT KIK USER: Yes. Or you can do a mirror pic

OCE: Ohhh thats a good idea!

SUSPECT KIK USER: Can you do that?

OCE: What should i show?!

SUSPECT KIK USER: Well you said you were naked..just show your breasts

OCE: That's it?? [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: Well I'm sure your whole body would be just as easy

OCE: Lol it's a big mirror lol

SUSPECT KIK USER: Okay nice. Okay then…show me all of you

OCE: What should i do? Naked?! [Smiling Blushing Emoji]

SUSPECT KIK USER: Hmm sure

OCE: Pic or vid?

SUSPECT KIK USER: Pic

OCE: Okkkk

17. At this point in the conversation, the SUSPECT KIK USER sends a short video of an adult male, naked, wearing white socks, masturbating a naked erect penis. The OCE asks if that is him right now and the SUSPECT KIK USER replies, "Yes". The OCE asks, "Thinking of me?!" and the SUSPECT KIK USER replies, "Oh yes mmm". The conversation continues as follows:

SUSPECT KIK USER: I'm just thinking of what it would be like to have you here. Are you doing a pic

OCE: Meeee tooooo. I'm trying to look cute

SUSPECT KIK USER: Oh I'm sure you look fine however. Madi [Smiling Emoji]

OCE: I dunnnno

SUSPECT KIK USER: Why not. Are you too nervous?

OCE: Nooo just trying to look nice

SUSPECT KIK USER: Okay. I think you look great always

OCE: Awww u do???

SUSPECT KIK USER: Yes def. So you have noting to worry about. Hey

OCE: Hiii

SUSPECT KIK USER: Hmm..no pic yet?

OCE: Sry I'm just nervous. I shouldn't be so I feel so dumb. I'm worried [u] won't like it

SUSPECT KIK USER: Oh I'm sure I'd like it

OCE: And my mom just texted and she's almost home so I think I'm nervous because of that. If she catches me she'll take my phone

SUSPECT KIK USER: Can I see? Delete the pic when you send it. It will be in your pictures

OCE: Okkkk. Omg she's home. She's calling me!

SUSPECT KIK USER: Okay

OCE: Brb. I'm sry [Upset Emoji]

SUSPECT KIK USER: Alright

18. Records obtained from Yahoo provided subscriber information for email address yahoo.com' provided a verified telephone number associated with the subscriber information to be -4241 and a Registration IP address of 73.142.155.80.

19. Records obtained from Verizon indicate that the telephone number 4241 is associated with an account held in the name of Stuart L. Adams, with a current billing address of 1465 Hooksett Rd, Unit 1358, Hooksett, New Hampshire 03106 (the SUBJECT PREMISES).

20. Records obtained from Kik from 10/6/2020 – 11/16/2020 for username 3003" show a Registration IP address of 73.142.155.80.

21. Records obtained from Comcast for the subscriber of the IP address 73.142.155.80 from August 2020 through November 2020 confirm that the IP address is assigned to Stuart Adams, with a service address of 1465 Hooksett Road, Unit 1358, Hooksett, NH 03106.

22. Through an inquiry of the New Hampshire Department of Safety – Division of Motor Vehicles ("DMV") database, the FBI was able to further identity Stuart L. Adams's year of birth as 1961, making him 59 years old, as well as the residence of Adams as 1465 Hooksett Rd, Unit 1358, Hooksett, New Hampshire 03106, near Manchester, New Hampshire.

23. I reviewed the photograph of Adams in the DMV database, as well as the photographs or "profile picture," associated with the SUSPECT KIK USER's profile in the Kik app. I also reviewed the photographs that the SUSPECT KIK USER sent within the chats with the OCE. I believe that they all depict the same person.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has

been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents

automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

26. As set forth above, probable cause exists to believe that an individual at the SUBJECT PREMISES has knowingly attempted to transfer obscene material to a minor who has not attained the age of 16.

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is <u>not</u>

present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

29. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of

the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

31. This warrant seeks authorization for law enforcement to compel STUART ADAMS to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on

certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front- facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

37. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

39. In light of the foregoing, and with respect to (1) any device found on STUART ADAMS' person; (2) any device found in STUART ADAMS' vehicle; (3) any device found in SUBJECT PREMISES reasonably believed to be owned, used, or accessed by STUART ADAMS'; law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of STUART ADAMS' to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of STUART ADAMS' and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of STUART ADAMS' and activate the iris recognition feature, for

the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

40. The proposed warrant does not authorize law enforcement to compel that an individual present at the SUBJECT PRESMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the SUBJECT PRESMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

41. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that on or about October 20, 2020, Stuart Adams, attempted to transfer obscene material to an individual who had not attained the age of 16 years, in violation of 18 U.S.C. § 1470. I therefore seek a warrant to search the SUBJECT PREMISES described in Attachment A and any computer and electronic media located therein, and to seize the items described in Attachment B.

42. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ Tarah Rankins
Tarah Rankins
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Nov 18, 2020

Time: 5:08 PM, Nov 18, 2020

/s/ Andrea K. Johnstone
Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched include:

1. the residential property located at 1465 Hooksett Road #1358 Hooksett, New Hampshire.
2. the person of STUART ADAMS.
3. One 2020 gray Chevrolet Silverado with New Hampshire registration 90

The SUBJECT PREMISES includes an attached townhouse. The following photograph depicts the SUBJECT PREMISES.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, 1470:

1. A tan rug/mat with a red and black checkered border

2. Visual depictions of obscene material including pictures of male genitals.

3. Any electronics that have access to the internet, the ability to create images, download applications, or have memory or history files including, but not limited to, mobile phones, smart phone, tablets, laptops, watches, and blue tooth devices for the following:

    a. Information establishing possession, identity of individuals, access to, or transmission or attempted transmission through interstate or foreign commerce, of obscene material to a minor;

    b. Correspondence related to the transfer or attempted transfer of obscene material to a minor, including, but not limited to, electronic mail, chat logs, electronic messages, text messages;

    c. All communications and files with or about potential minors involving sexual topics in the context of sending, or attempting to send the minor obscene material;

4. Records evidencing ownership and use of the items seized, including any and all lists of names, telephone numbers, addresses and contacts, and the content of voice mails and text messages and internet based applications including but not limited to:

    a. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

    b. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

    c. Documents and records regarding the ownership and/or possession of the searched premises.

6. Any and all security devices, to include encryption devices, needed to gain access to the electronic devices seized, including but not limited to:

   a. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data.

   b. Data security devices may consist of hardware, software, or other programming code.

   c. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

In searching the data, the computer personnel may examine and copy all of the data contained in the subject item to view their precise contents and determine whether the data falls within the items to be seized. In addition, the examining personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

The above seizure of computer and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

DEVICE UNLOCK: During the execution of the search of the property, person, and vehicle described in Attachment A, and with respect to (1) any device on STUART ADAMS' person; (2) any device found in SUBJECT PREMISES reasonably believed to be owned, used, or accessed by STUART ADAMS'; law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of STUART ADAMS' to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of STUART ADAMS' and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of STUART ADAMS' and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).